UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FREE SPEECH COALITION, INC., et al., Plaintiffs, v. ANGELA COLMENERO, In Her Official Capacity As Interim Attorney General For The State Of Texas Defendant.	**CASE NO. 1:23-cv-00917-DAE**

REBUTTAL DECLARATION OF RICHARD L. SONNIER III IN SUPPORT OF PLAINTIFFS' MOTION FOR EXPEDITED PRELIMINARY INJUNCTION

I, Richard L Sonnier III, declare as follows:

1. I have been retained by Plaintiffs in the above captioned matter to provide technical expertise in the areas of Internet technologies and operations including age verification of users, content filtering, parental controls, family safe usage, the cost of implementing Internet technologies, the cost of operating Internet technologies, Internet privacy, Internet standards, cybersecurity, and Internet regulations.

2. I have reviewed Defendant's Opposition, as well as the Declarations of Erik Cabrera and Tony Allen.

3. Mr. Cabrera states that he had trouble reproducing my results with the Bing search engine. Cabrera Decl. at ¶ 4. On a second computer, I performed the procedure described in my previous declaration with the Bing search engine and confirmed my results. I cannot speculate about why Mr. Cabrera observed blurred images in his search results, but I am happy to assist Mr. Cabrera in replicating my results.

4. Also, Mr. Cabrera states "the vast majority of results—almost all—were for Pornhub.com, XNXX.com, xhamster.com, and xvideos.com." Cabrera Decl. at ¶ 5. I ran a search on Bing for "sucks cock," and the resulting images were from primarily eporner.com, xbabe.com, and mylust.com. The video results included videos from xhamster.com and spankbang.com.

5. The Opposition brief states (Opp. at p. 12): "According to their declarant, Richard L. Sonnier, a child could search Bing.com for 'hot sex' and instantly gain access to porn that way. Dkt. 5-2. But the websites and videos that populate from that search are porn websites that would be subject to HB 1181. Notably, under current conditions, the vast majority—if not all—of the results are Plaintiffs' websites."

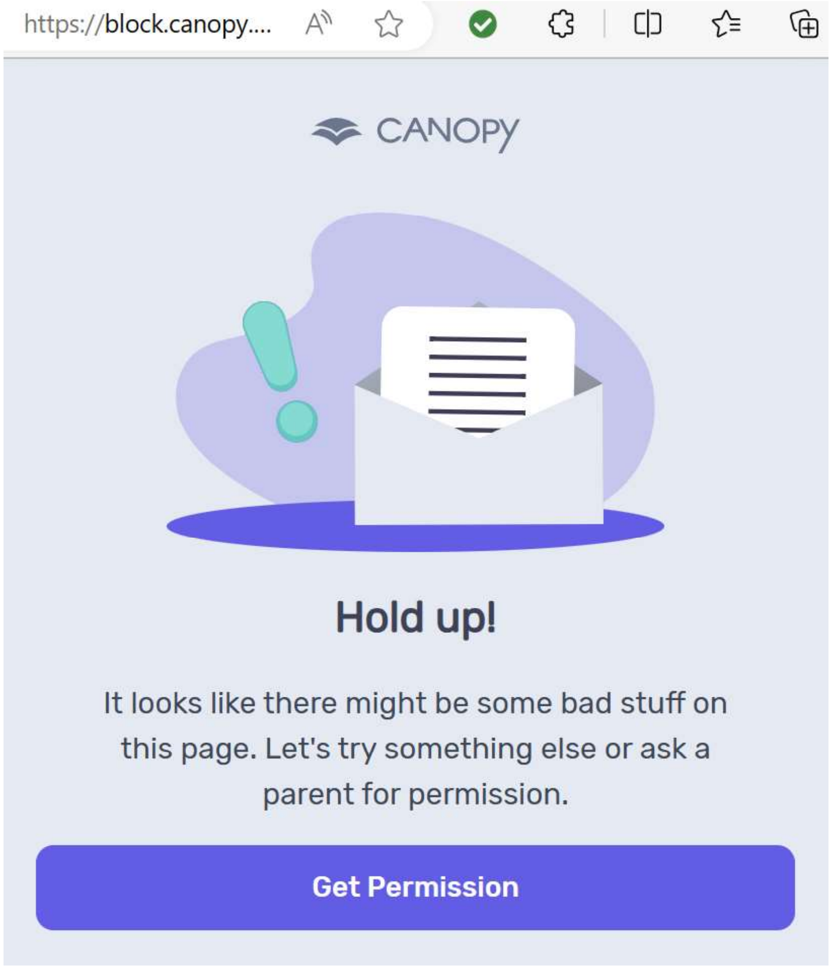
6. If the above-quoted statement implies that age verification protocols would change the search results from search engines so that explicit images and videos from adult websites would no longer appear in the search results, then the Defendant is mistaken due to the way search engines operate. When a search engine scans a website, which is a routine process, it captures the images and videos on that website regardless of any age verification protocols on

that website that might prevent a human user from accessing that website. Any website that wants to be in search engine results must be configured to follow search engine procedures. One such procedure is to distinguish between human users and search engine scans when accessing the website. For example, Bing explains how to do this for the Bing search engine. *See* https://www.bing.com/webmasters/help/which-crawlers-does-bing-use-8c184ec0. Indeed, search engine scans are automated, userless, machine-run processes without "ages" so that age verification protocols cannot work. When responding to a search by a user, the search engine sends the previously captured images or videos to the user in the search results without contacting the original website from which the images or videos were captured. As a result, any age verification protocols on the original website do not apply to the search engine results.

7. Mr. Allen refers to survey studies to support his claim that filtering is an "ineffective mechanism." Allen Decl. at ¶ 76. For example, Mr. Allen refers to an Oxford study by Przybylski and Nash. I reviewed that reference; and it does not find that Internet content filtering technology does not work (below I will explain that it absolutely does work), rather it reaches a social science statistical analysis that this known-to-work technology is not being implemented properly within UK and EU society.

8. Content filtering software for parents is actually an implementation of a general technology at work across the Internet. In general, Internet content filtering is simply indexing by category or keyword the context of the Internet, i.e., websites; and then allowing users to use that index to see what they want or to block what they do not want. Internet content filtering is what Bing does, for example. When I and Mr. Cabrera turned Bing's "SafeSearch" function on and off, we were doing Internet content filtering; and both of us have confirmed that it absolutely works. Furthermore, parental control applications that expand upon Internet content filtering work as well. I have personally confirmed the effectiveness of the parental control application called Canopy.

9. To do this, I went to the canopy website (canopy.us) and clicked on the "Start Free Trial" button. I provided an email address and entered my own password exceeding Canopy's password requirements. Next, I selected one of Canopy's subscription plans. I chose the mid-level plan. I entered a credit card. As part of the free trial, the first seven days are free. This created my account and placed me directly into a web console where I could start protecting my devices. I added two devices. One was a Windows PC, and the other an Android smart phone. Then I repeated the procedure from my First Declaration on the Bing search engine with the search terms "hot sex." I received the following instead of my previous results:



Hold up!

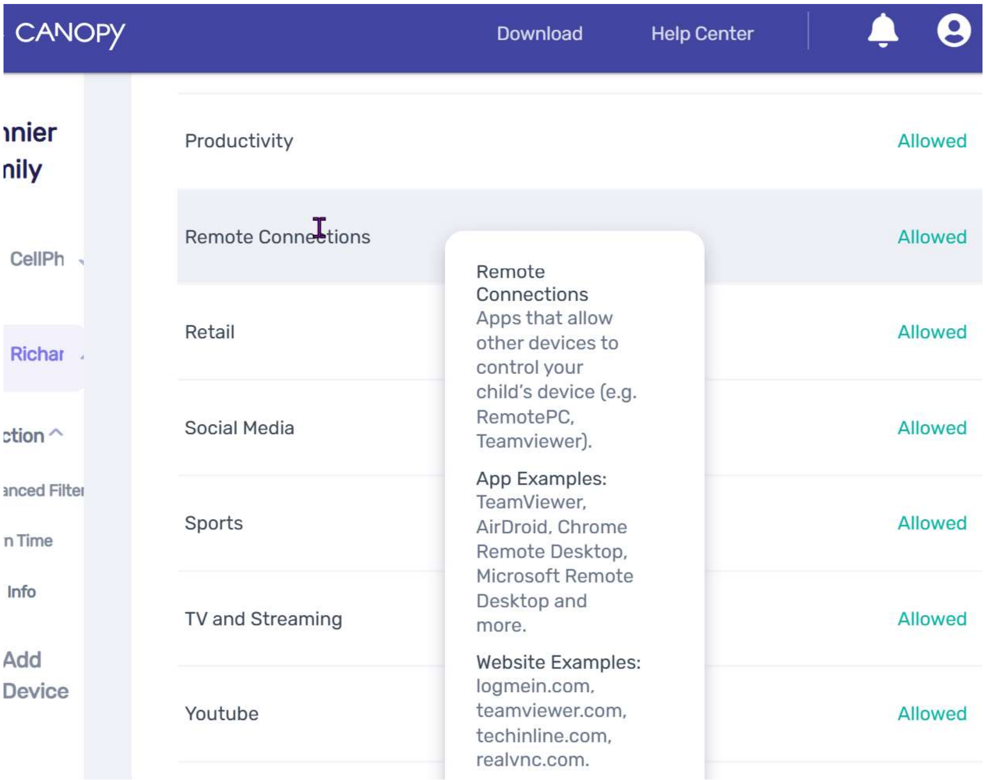
It looks like there might be some bad stuff on this page. Let's try something else or ask a parent for permission.

10. In my previous declaration, I discussed that one advantage of parental control applications is their ability to tune the protection to specific preferences. Here, Canopy automatically forced Bing's "SafeSearch" function to "strict," blocking explicit sexual material. However, for older teenagers, Canopy allows parents to grant permission if desired.

11. Canopy allows parents to permit access to social media sites while still blocking explicit sexual content. For example, I was able to go to the social media site Reddit, https://www.reddit.com/t/nfl/, while Canopy was installed. I then tried to enter a "subreddit" containing sexually explicit material, https://www.reddit.com/r/gonewild/. Although Canopy did not block the Reddit page banner that included a sexually explicit image, it blocked every sexually explicit image within the subreddit thread posted by Reddit users, as I saw when I scrolled down several days' worth of posts.

12. Canopy blocked access to Pornhub.com, xnxx.com, and other sites operated by the Plaintiffs in this action.

13. Also, I found that Canopy blocks the Tor Browser, described in my previous declaration, and prevents it from connecting to the Tor network. Additionally, Canopy blocks alternative web browsers like Brave that can circumvent its protections. While it does not block them by default, Canopy allows parents to block remote desktop applications like TeamViewer:



Productivity	Allowed
Remote Connections	Allowed
Retail	Allowed
Social Media	Allowed
Sports	Allowed
TV and Streaming	Allowed
Youtube	Allowed

Remote Connections
Apps that allow other devices to control your child's device (e.g. RemotePC, Teamviewer).

App Examples:
TeamViewer, AirDroid, Chrome Remote Desktop, Microsoft Remote Desktop and more.

Website Examples:
logmein.com, teamviewer.com, techinline.com, realvnc.com.

14. Canopy's installation procedure recommends as a default to install it so that it cannot be uninstalled by the user unless the parent approves it. The parent can override that

configuration during the installation process if they wish or they can turn that configuration on or off at any time in the Canopy's web console.

15. In my opinion, the Canopy setup and installation on devices was simple, and within the skill level of any computer-using adult, and automatically performs many security configurations that would otherwise be confusing to the average computer user.

16. Finally, Mr. Allen states that "DNS filtering fails when 'DNS over HTTPS' is used to cloak a user's usage. This is easily adopted and has been standard for US users since 2019 if they use a Firefox/Mozilla Browser, so this control is easily circumvented." Allen Decl. at ¶ 74. It is not correct that this feature circumvents parental control software. The same source that Mr. Allen refers to, https://support.mozilla.org/en-US/kb/firefox-dns-over-https (attached as Exhibit 1), which is consistent with my understanding, explains that Firefox is configured to work with parental control software, so that when Firefox detects such software, it disables the DNS-over-HTTPS feature.

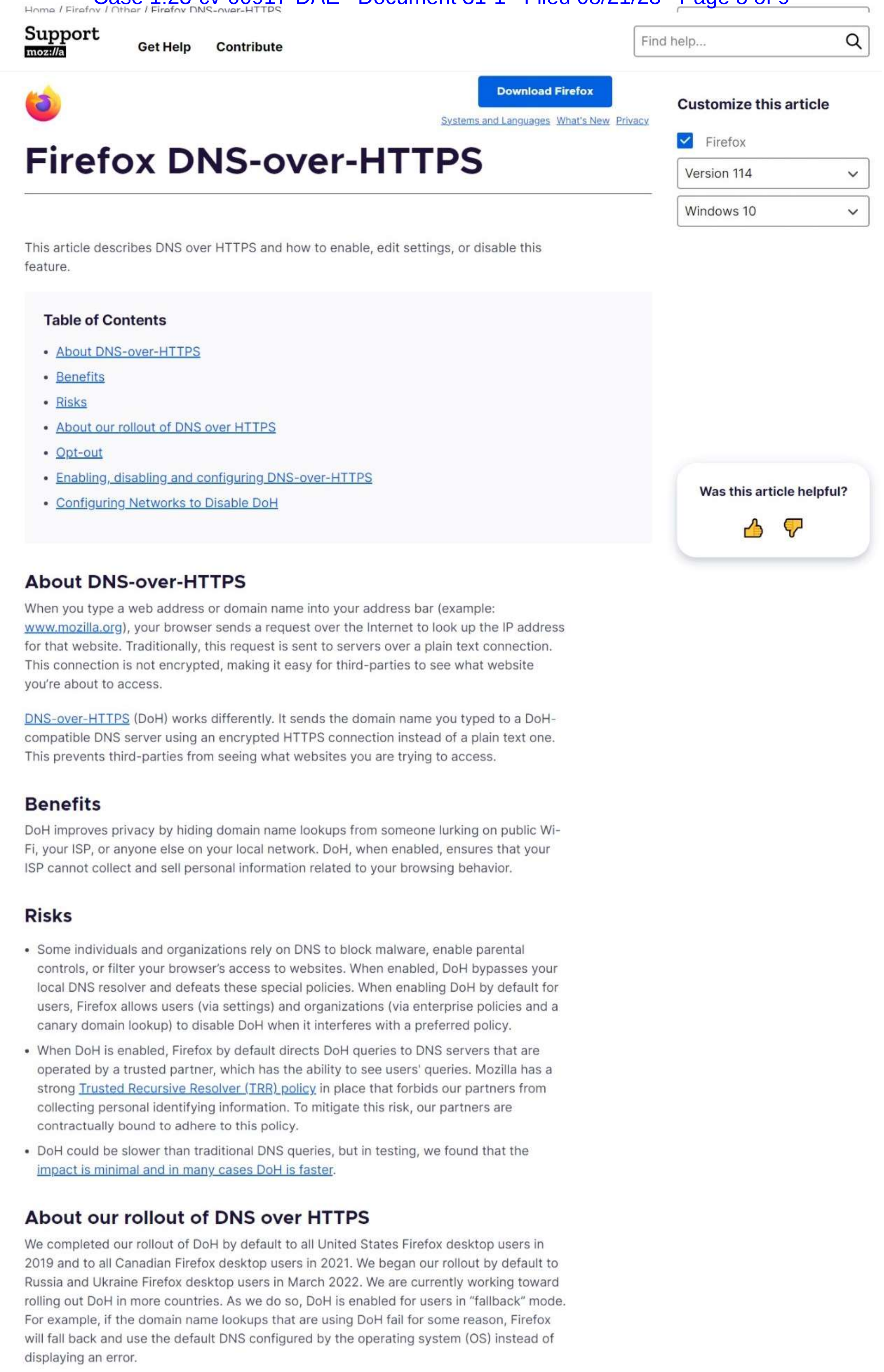
I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 21st day of August 2023 in Houston, Texas.

Richard L Sonnier III

RICHARD L SONNIER III

EXHIBIT 1



Firefox DNS-over-HTTPS

This article describes DNS over HTTPS and how to enable, edit settings, or disable this feature.

Table of Contents

About DNS-over-HTTPS

When you type a web address or domain name into your address bar (example: www.mozilla.org), your browser sends a request over the Internet to look up the IP address for that website. Traditionally, this request is sent to servers over a plain text connection. This connection is not encrypted, making it easy for third-parties to see what website you're about to access.

DNS-over-HTTPS (DoH) works differently. It sends the domain name you typed to a DoH-compatible DNS server using an encrypted HTTPS connection instead of a plain text one. This prevents third-parties from seeing what websites you are trying to access.

Benefits

DoH improves privacy by hiding domain name lookups from someone lurking on public Wi-Fi, your ISP, or anyone else on your local network. DoH, when enabled, ensures that your ISP cannot collect and sell personal information related to your browsing behavior.

Risks

- Some individuals and organizations rely on DNS to block malware, enable parental controls, or filter your browser's access to websites. When enabled, DoH bypasses your local DNS resolver and defeats these special policies. When enabling DoH by default for users, Firefox allows users (via settings) and organizations (via enterprise policies and a canary domain lookup) to disable DoH when it interferes with a preferred policy.
- When DoH is enabled, Firefox by default directs DoH queries to DNS servers that are operated by a trusted partner, which has the ability to see users' queries. Mozilla has a strong Trusted Recursive Resolver (TRR) policy in place that forbids our partners from collecting personal identifying information. To mitigate this risk, our partners are contractually bound to adhere to this policy.
- DoH could be slower than traditional DNS queries, but in testing, we found that the impact is minimal and in many cases DoH is faster.

About our rollout of DNS over HTTPS

We completed our rollout of DoH by default to all United States Firefox desktop users in 2019 and to all Canadian Firefox desktop users in 2021. We began our rollout by default to Russia and Ukraine Firefox desktop users in March 2022. We are currently working toward rolling out DoH in more countries. As we do so, DoH is enabled for users in "fallback" mode. For example, if the domain name lookups that are using DoH fail for some reason, Firefox will fall back and use the default DNS configured by the operating system (OS) instead of displaying an error.

Opt-out

If you're an existing Firefox user in a locale where we've rolled out DoH by default, you'll receive a notification in Firefox if and when DoH is first enabled, allowing you to choose not to use DoH and instead continue using your default OS DNS resolver.

In addition, Firefox will check for certain functions that might be affected if DoH is enabled, including:

- Are parental controls enabled?
- Is the default DNS server filtering potentially malicious content?
- Is the device managed by an organization that might have a special DNS configuration?

If any of these tests determine that DoH might interfere with the function, DoH will not be enabled. These tests will run every time the device connects to a different network.

Enabling, disabling and configuring DNS-over-HTTPS

See the Configure DNS over HTTPS protection levels in Firefox article.

Configuring Networks to Disable DoH

- Configuring Networks to Disable DNS over HTTPS
- DNS-over-HTTPS (DoH) FAQs

Share this article: https://mzl.la/3pbH2so

These fine people helped write this article:

AliceWyman, Michele Rodaro, Mozinet, Wesley Branton, Joni, Paul, Marcelo Ghelman, Lamont Gardenhire, Angela Lazar, Fabi, Bithiah, Denys

Volunteer

Grow and share your expertise with others. Answer questions and improve our knowledge base.

Learn More

Mozilla

Report Trademark Abuse

Source code

Twitter

Join our Community

Explore Help Articles

Firefox

Download

Firefox Desktop

Android Browser

iOS Browser

Focus Browser

Firefox for Developers

Developer Edition

Beta

Beta for Android

Nightly

Nightly for Android

Firefox Accounts

Sign In/Up

Benefits

Firefox Private Network

Language

English

moz://a

mozilla.org Terms of Service Privacy Cookies Contact

Visit Mozilla Corporation's not-for-profit parent, the Mozilla Foundation.